

CLAIMS

What is claimed is:

- 1 1. A method comprising:
 - 2 writing a party's authenticating information and a first digital certificate issuing
 - 3 authority's authenticating information in an electronic document;
 - 4 signing the electronic document to obtain a once signed electronic document; and
 - 5 transmitting the once signed electronic document to a second digital certificate
 - 6 issuing authority to obtain a twice signed electronic document.
- 1 2. The method of claim 1 wherein signing the electronic document to obtain a once
2 signed electronic document comprises:
 - 3 obtaining a hash value using contents of the electronic document as input to a
 - 4 hash algorithm;
 - 5 encrypting the hash value using the first digital certificate issuing authority's
 - 6 private key; and
 - 7 storing the encrypted hash value in the electronic document.
- 1 3. The method of claim 1 wherein obtaining a twice signed electronic document
2 comprises at least one of the second digital certificate issuing authority inserting its
3 authenticating information in the once signed electronic document, obtaining a hash value
4 using contents of the electronic document as input to a hash algorithm, encrypting the

5 hash value using the second digital certificate issuing authority's private key, including
6 the encrypted hash value in the electronic document, and transmitting the twice signed
7 electronic document.

1 4. The method of claim 3 wherein obtaining a hash value using contents of the
2 electronic document as input to a hash algorithm comprises at least one of, using the
3 party's authenticating information, using the first digital certificate issuing authority's
4 authenticating information, using the digital signature of the first digital certificate
5 issuing authority, and using the second digital certificate issuing authority's
6 authenticating information as input to a hash algorithm.

1 5. The method of claim 1, wherein writing a party's authenticating information and a
2 first digital certificate issuing authority's authenticating information in an electronic
3 document comprises receiving the party's authenticating information via a secure
4 connection.

1 6. A computer system comprising:
2 a bus;
3 a data storage device coupled to said bus; and
4 a processor coupled to said data storage device, said processor operable to receive
5 instructions which, when executed by the processor, cause the processor to perform a
6 method comprising writing a party's authenticating information and a first digital
7 certificate issuing authority's authenticating information in an electronic document;

8 signing the electronic document to obtain a once signed electronic document; and
9 transmitting the once signed electronic document to a second digital certificate
10 issuing authority to obtain a twice signed electronic document.

1 7. A computer system as in claim 6 wherein signing the electronic document to
2 obtain a once signed electronic document comprises:

3 obtaining a hash value using contents of the electronic document as input to a
4 hash algorithm;

5 encrypting the hash value using the first digital certificate issuing authority's
6 private key; and

7 storing the encrypted hash value in the electronic document.

1 8. A computer system as in claim 6 wherein obtaining a twice signed electronic
2 document comprises at least one of the second digital certificate issuing authority
3 inserting its authenticating information in the once signed electronic document, obtaining
4 a hash value using contents of the electronic document as input to a hash algorithm,
5 encrypting the hash value using the second digital certificate issuing authority's private
6 key, including the encrypted hash value in the electronic document, and transmitting the
7 twice signed electronic document.

1 9. A computer system as in claim 8 wherein obtaining a hash value using contents of
2 the electronic document as input to a hash algorithm comprises at least one of, using the
3 party's authenticating information, using the first digital certificate issuing authority's

- 4 authenticating information, using the digital signature of the first digital certificate
- 5 issuing authority, and using the second digital certificate issuing authority's
- 6 authenticating information as input to a hash algorithm.

1 10. A computer system as in claim 6 wherein writing a party's authenticating
2 information and a first digital certificate issuing authorities authenticating information in
3 an electronic document comprises receiving the party's authenticating information via a
4 secure connection.

1 11. An article of manufacture comprising:
2 a machine-accessible medium including instructions that, when executed by a
3 machine, causes the machine to perform operations comprising
4 writing a party's authenticating information and a first digital certificate issuing
5 authorities authenticating information in an electronic document;
6 signing the electronic document to obtain a once signed electronic document; and
7 transmitting the once signed electronic document to a second digital certificate
8 issuing authority to obtain a twice signed electronic document.

1 12. An article of manufacture as in claim 11 wherein signing the electronic document
2 to obtain a once signed electronic document comprises:
3 obtaining a hash value using contents of the electronic document as input to a
4 hash algorithm;

5 encrypting the hash value using the first digital certificate issuing authority's
6 private key; and
7 storing the encrypted hash value in the electronic document.

1 13. An article of manufacture as in claim 11 wherein obtaining a twice signed
2 electronic document comprises at least one of the second digital certificate issuing
3 authority inserting its authenticating information in the once signed electronic document,
4 obtaining a hash value using contents of the electronic document as input to a hash
5 algorithm, encrypting the hash value using the second digital certificate issuing
6 authority's private key, including the encrypted hash value in the electronic document,
7 and transmitting the twice signed electronic document.

1 14. An article of manufacture as in claim 13 wherein obtaining a hash value using
2 contents of the electronic document as input to a hash algorithm comprises at least one of,
3 using the party's authenticating information, using the first digital certificate issuing
4 authorities authenticating information, using the digital signature of the first digital
5 certificate issuing authority, and using the second digital certificate issuing authority's
6 authenticating information as input to a hash algorithm.

1 15. An article of manufacture as in claim 11 wherein writing a party's authenticating
2 information and a first digital certificate issuing authorities authenticating information in
3 an electronic document comprises receiving the party's authenticating information via a
4 secure connection.

1 16. A method comprising:
2 receiving a once signed electronic document;
3 writing a digital certificate issuing authority's authenticating information in the once
4 signed electronic document;
5 signing the once signed electronic document to form a twice signed electronic document;
6 and
7 transmitting the twice signed electronic document.

1 17. The method of claim 16 wherein signing the once signed electronic document to
2 form a twice signed electronic document comprises:
3 obtaining a hash value using contents of the once signed electronic document and
4 using the digital certificate issuing authority's authenticating information as input to a
5 hash algorithm;
6 encrypting the hash value using the digital certificate issuing authority's private
7 key; and
8 writing the encrypted hash value in the electronic document.

1 18. A computer system comprising:
2 a bus;
3 a data storage device coupled to said bus; and
4 a processor coupled to said data storage device, said processor operable to receive
5 instructions which, when executed by the processor, cause the processor to perform a
6 method comprising receiving a once signed electronic document;

- 7 writing a digital certificate issuing authority's authenticating information in the once
- 8 signed electronic document;
- 9 signing the once signed electronic document to form a twice signed electronic document;
- 10 and
- 11 transmitting the twice signed electronic document.

- 1 19. A computer system as in claim 18 wherein signing the once signed electronic
- 2 document to form a twice signed electronic document comprises:
 - 3 obtaining a hash value using contents of the once signed electronic document and
 - 4 using the digital certificate issuing authority's authenticating information as input to a
 - 5 hash algorithm;
 - 6 encrypting the hash value using the digital certificate issuing authority's private
 - 7 key; and
 - 8 writing the encrypted hash value in the electronic document.

- 1 20. An article of manufacture comprising:
 - 2 a machine-accessible medium including instructions that, when executed by a
 - 3 machine, causes the machine to perform operations comprising receiving a once signed
 - 4 electronic document;
 - 5 writing a digital certificate issuing authority's authenticating information in the
 - 6 once signed electronic document;
 - 7 signing the once signed electronic document to form a twice signed electronic
 - 8 document; and

transmitting the twice signed electronic document.

21. An article of manufacture as in claim 20 wherein signing the once signed electronic document to form a twice signed electronic document comprises:

obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information as input to a hash algorithm;

encrypting the hash value using the digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.